AMENDMENT NO. CAL. NO.

October 15, 2002

Purpose: To provide for cyber security research and development.

IN THE SENATE OF THE UNITED STATES—107TH Cong., 2D Sess.

S. 2182, 107TH Congress, 2D Session

OCTOBER ——, 2002

( ) Referred to the Committee on ———————— and ordered to be printed

( ) Ordered to lie on the table and to be printed

INTENDED to be proposed by Mr. WYDEN (for himself and Mr. ALLEN)

Viz: Strike out all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Cyber Security Research and Development Act''.

SEC. 2. FINDINGS.

The Congress finds the following:

(1) Revolutionary advancements in computing and communications technology have interconnected government, commercial, scientific, and educational

infrastructures—including critical infrastructures for electric power, natural gas and petroleum production and distribution, telecommunications, transportation, water supply, banking and finance, and emergency and government services—in a vast, interdependent physical and electronic network.

(2) Exponential increases in interconnectivity have facilitated enhanced communications, economic growth, and the delivery of services critical to the public welfare, but have also increased the consequences of temporary or prolonged failure.

(3) A Department of Defense Joint Task Force concluded after a 1997 United States information warfare exercise that the results ''clearly demonstrated our lack of preparation for a coordinated cyber and physical attack on our critical military and civilian infrastructure''.

(4) Computer security technology and systems implementation lack—

(A) sufficient long term research funding;

(B) adequate coordination across Federal and State government agencies and among government, academia, and industry; and

(C) sufficient numbers of outstanding researchers in the field.

(5) Accordingly, Federal investment in computer and network security research and development must be significantly increased to—

(A) improve vulnerability assessment and technological and systems solutions;

(B) expand and improve the pool of information security professionals, including researchers, in the United States workforce; and

(C) better coordinate information sharing and collaboration among industry, government, and academic research projects.

(6) While African-Americans, Hispanics, and Native Americans constitute 25 percent of the total United States workforce and 30 percent of the college-age population, members of these minorities comprise less than 7 percent of the United States computer and information science workforce.

SEC. 3. DEFINITIONS.

In this Act:

(1) DIRECTOR.—The term ''Director'' means the Director of the National Science Foundation.

(2) INSTITUTION OF HIGHER EDUCATION.—The term ''institution of higher education'' has the meaning given that term in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)).

SEC. 4. NATIONAL SCIENCE FOUNDATION RESEARCH.

(a) COMPUTER AND NETWORK SECURITY RESEARCH GRANTS.—

(1) IN GENERAL.—The Director shall award grants for basic research on innovative approaches to the structure of computer and network hardware and software that are aimed at enhancing computer security. Research areas may include—

(A) authentication, cryptography, and other secure data communications technology;

(B) computer forensics and intrusion detection;

(C) reliability of computer and network applications, middleware, operating systems, control systems, and communications infrastructure;

(D) privacy and confidentiality;

(E) network security architecture, including tools for security administration and analysis;

(F) emerging threats;

(G) vulnerability assessments and techniques for quantifying risk;

(H) remote access and wireless security; and

(I) enhancement of law enforcement ability to detect, investigate, and prosecute cybercrimes, including those that involve piracy of intellectual property.

(2) MERIT REVIEW; COMPETITION.—Grants shall be awarded under this section on a merit-reviewed competitive basis.

(3) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $35,000,000 for fiscal year 2003;

(B) $40,000,000 for fiscal year 2004;

(C) $46,000,000 for fiscal year 2005;

(D) $52,000,000 for fiscal year 2006; and

(E) $60,000,000 for fiscal year 2007.

(b) COMPUTER AND NETWORK SECURITY RESEARCH CENTERS.—

(1) IN GENERAL.—The Director shall award multiyear grants, subject to the availability of appropriations, to institutions of higher education, nonprofit research institutions, or consortia thereof to establish multidisciplinary Centers for Computer and Network Security Research. Institutions of higher education, nonprofit research institutions, or con-

sortia thereof receiving such grants may partner with 1 or more government laboratories or for-profit institutions, or other institutions of higher education or nonprofit research institutions.

(2) MERIT REVIEW; COMPETITION.—Grants shall be awarded under this subsection on a merit-reviewed competitive basis.

(3) PURPOSE.—The purpose of the Centers shall be to generate innovative approaches to computer and network security by conducting cutting-edge, multidisciplinary research in computer and network security, including the research areas described in subsection (a)(1).

(4) APPLICATIONS.—An institution of higher education, nonprofit research institution, or consortia thereof seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

(A) the research projects that will be undertaken by the Center and the contributions of each of the participating entities;

(B) how the Center will promote active collaboration among scientists and engineers from

different disciplines, such as computer scientists, engineers, mathematicians, and social science researchers;

(C) how the Center will contribute to increasing the number and quality of computer and network security researchers and other professionals, including individuals from groups historically underrepresented in these fields; and

(D) how the center will disseminate research results quickly and widely to improve cyber security in information technology networks, products, and services.

(5) CRITERIA.—In evaluating the applications submitted under paragraph (4), the Director shall consider, at a minimum—

(A) the ability of the applicant to generate innovative approaches to computer and network security and effectively carry out the research program;

(B) the experience of the applicant in conducting research on computer and network security and the capacity of the applicant to foster new multidisciplinary collaborations;

(C) the capacity of the applicant to attract and provide adequate support for a diverse group of undergraduate and graduate students and postdoctoral fellows to pursue computer and network security research; and

(D) the extent to which the applicant will partner with government laboratories, for-profit entities, other institutions of higher education, or nonprofit research institutions, and the role the partners will play in the research undertaken by the Center.

(6) ANNUAL MEETING.—The Director shall convene an annual meeting of the Centers in order to foster collaboration and communication between Center participants.

(7) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for the National Science Foundation to carry out this subsection—

(A) $12,000,000 for fiscal year 2003;

(B) $24,000,000 for fiscal year 2004;

(C) $36,000,000 for fiscal year 2005;

(D) $36,000,000 for fiscal year 2006; and

(E) $36,000,000 for fiscal year 2007.

SEC. 5. NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY PROGRAMS.

(a) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—

(1) IN GENERAL.—The Director shall establish a program to award grants to institutions of higher education (or consortia thereof) to establish or improve undergraduate and master's degree programs in computer and network security, to increase the number of students, including the number of students from groups historically underrepresented in these fields, who pursue undergraduate or master's degrees in fields related to computer and network security, and to provide students with experience in government or industry related to their computer and network security studies.

(2) MERIT REVIEW.—Grants shall be awarded under this subsection on a merit-reviewed competitive basis.

(3) USE OF FUNDS.—Grants awarded under this subsection shall be used for activities that enhance the ability of an institution of higher education (or consortium thereof) to provide high-quality undergraduate and master's degree programs in computer and network security and to recruit and

retain increased numbers of students to such programs. Activities may include—

(A) revising curriculum to better prepare undergraduate and master's degree students for careers in computer and network security;

(B) establishing degree and certificate programs in computer and network security;

(C) creating opportunities for undergraduate students to participate in computer and network security research projects;

(D) acquiring equipment necessary for student instruction in computer and network security, including the installation of testbed networks for student use;

(E) providing opportunities for faculty to work with local or Federal Government agencies, private industry, nonprofit research institutions, or other academic institutions to develop new expertise or to formulate new research directions in computer and network security;

(F) establishing collaborations with other academic institutions or academic departments that seek to establish, expand, or enhance programs in computer and network security;

(G) establishing student internships in computer and network security at government agencies or in private industry;

(H) establishing collaborations with other academic institutions to establish or enhance a web-based collection of computer and network security courseware and laboratory exercises for sharing with other institutions of higher education, including community colleges;

(I) establishing or enhancing bridge programs in computer and network security between community colleges and universities; and

(K) any other activities the Director determines will accomplish the goals of this subsection.

(4) SELECTION PROCESS.—

(A) APPLICATION.—An institution of higher education (or a consortium thereof) seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum—

(i) a description of the applicant's computer and network security research

and instructional capacity, and in the case of an application from a consortium of institutions of higher education, a description of the role that each member will play in implementing the proposal;

(ii) a comprehensive plan by which the institution or consortium will build instructional capacity in computer and information security;

(iii) a description of relevant collaborations with government agencies or private industry that inform the instructional program in computer and network security;

(iv) a survey of the applicant's historic student enrollment and placement data in fields related to computer and network security and a study of potential enrollment and placement for students enrolled in the proposed computer and network security program; and

(v) a plan to evaluate the success of the proposed computer and network security program, including post-graduation assessment of graduate school and job place-

ment and retention rates as well as the relevance of the instructional program to graduate study and to the workplace.

(B) AWARDS.—(i) The Director shall ensure, to the extent practicable, that grants are awarded under this subsection in a wide range of geographic areas and categories of institutions of higher education, including minority serving institutions.

(ii) The Director shall award grants under this subsection for a period not to exceed 5 years.

(5) ASSESSMENT REQUIRED.—The Director shall evaluate the program established under this subsection no later than 6 years after the establishment of the program. At a minimum, the Director shall evaluate the extent to which the program achieved its objectives of increasing the quality and quantity of students, including students from groups historically underrepresented in computer and network security related disciplines, pursuing undergraduate or master's degrees in computer and network security.

(6) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Na-

tional Science Foundation to carry out this subsection—

(A) $15,000,000 for fiscal year 2003;

(B) $20,000,000 for fiscal year 2004;

(C) $20,000,000 for fiscal year 2005;

(D) $20,000,000 for fiscal year 2006; and

(E) $20,000,000 for fiscal year 2007.

(b) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT OF 1992.—

(1) GRANTS.—The Director shall provide grants under the Scientific and Advanced Technology Act of 1992 (42 U.S.C. 1862i) for the purposes of section 3(a) and (b) of that Act, except that the activities supported pursuant to this subsection shall be limited to improving education in fields related to computer and network security.

(2) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $1,000,000 for fiscal year 2003;

(B) $1,250,000 for fiscal year 2004;

(C) $1,250,000 for fiscal year 2005;

(D) $1,250,000 for fiscal year 2006; and

(E) $1,250,000 for fiscal year 2007.

(c) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH.—

(1) IN GENERAL.—The Director shall establish a program to award grants to institutions of higher education to establish traineeship programs for graduate students who pursue computer and network security research leading to a doctorate degree by providing funding and other assistance, and by providing graduate students with research experience in government or industry related to the students' computer and network security studies.

(2) MERIT REVIEW.—Grants shall be provided under this subsection on a merit-reviewed competitive basis.

(3) USE OF FUNDS.—An institution of higher education shall use grant funds for the purposes of—

(A) providing traineeships to students who are citizens, nationals, or lawfully admitted permanent resident aliens of the United States and are pursuing research in computer or network security leading to a doctorate degree;

(B) paying tuition and fees for students receiving traineeships under subparagraph (A);

(C) establishing scientific internship programs for students receiving traineeships under subparagraph (A) in computer and network security at for-profit institutions, nonprofit research institutions, or government laboratories; and

(D) other costs associated with the administration of the program.

(4) TRAINEESHIP AMOUNT.—Traineeships provided under paragraph (3)(A) shall be in the amount of $25,000 per year, or the level of the National Science Foundation Graduate Research Fellowships, whichever is greater, for up to 3 years.

(5) SELECTION PROCESS.—An institution of higher education seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

(A) the instructional program and research opportunities in computer and network security available to graduate students at the applicant's institution; and

(B) the internship program to be established, including the opportunities that will be

made available to students for internships at for-profit institutions, nonprofit research institutions, and government laboratories.

(6) REVIEW OF APPLICATIONS.—In evaluating the applications submitted under paragraph (5), the Director shall consider—

(A) the ability of the applicant to effectively carry out the proposed program;

(B) the quality of the applicant's existing research and education programs;

(C) the likelihood that the program will recruit increased numbers of students, including students from groups historically underrepresented in computer and network security related disciplines, to pursue and earn doctorate degrees in computer and network security;

(D) the nature and quality of the internship program established through collaborations with government laboratories, nonprofit research institutions, and for-profit institutions;

(E) the integration of internship opportunities into graduate students' research; and

(F) the relevance of the proposed program to current and future computer and network security needs.

(7) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $10,000,000 for fiscal year 2003;

(B) $20,000,000 for fiscal year 2004;

(C) $20,000,000 for fiscal year 2005;

(D) $20,000,000 for fiscal year 2006; and

(E) $20,000,000 for fiscal year 2007.

(d) GRADUATE RESEARCH FELLOWSHIPS PROGRAM SUPPORT.—Computer and network security shall be included among the fields of specialization supported by the National Science Foundation's Graduate Research Fellowships program under section 10 of the National Science Foundation Act of 1950 (42 U.S.C. 1869).

(e) CYBER SECURITY FACULTY DEVELOPMENT TRAINEESHIP PROGRAM.—

(1) IN GENERAL.—The Director shall establish a program to award grants to institutions of higher education to establish traineeship programs to enable graduate students to pursue academic careers in cyber security upon completion of doctoral degrees.

(2) MERIT REVIEW; COMPETITION.—Grants shall be awarded under this section on a merit-reviewed competitive basis.

(3) APPLICATION.—Each institution of higher education desiring to receive a grant under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director shall require.

(4) USE OF FUNDS.—Funds received by an institution of higher education under this paragraph shall—

(A) be made available to individuals on a merit-reviewed competitive basis and in accordance with the requirements established in paragraph (7);

(B) be in an amount that is sufficient to cover annual tuition and fees for doctoral study at an institution of higher education for the duration of the graduate traineeship, and shall include, in addition, an annual living stipend of $25,000; and

(C) be provided to individuals for a duration of no more than 5 years, the specific duration of each graduate traineeship to be deter-

mined by the institution of higher education, on a case-by-case basis.

(5) REPAYMENT.—Each graduate traineeship shall—

(A) subject to paragraph (5)(B), be subject to full repayment upon completion of the doctoral degree according to a repayment schedule established and administered by the institution of higher education;

(B) be forgiven at the rate of 20 percent of the total amount of the graduate traineeship assistance received under this section for each academic year that a recipient is employed as a full-time faculty member at an institution of higher education for a period not to exceed 5 years; and

(C) be monitored by the institution of higher education receiving a grant under this subsection to ensure compliance with this subsection.

(6) EXCEPTIONS.—The Director may provide for the partial or total waiver or suspension of any service obligation or payment by an individual under this section whenever compliance by the individual is impossible or would involve extreme hardship to the

individual, or if enforcement of such obligation with respect to the individual would be unconscionable.

(7) ELIGIBILITY.—To be eligible to receive a graduate traineeship under this section, an individual shall—

(A) be a citizen, national, or lawfully admitted permanent resident alien of the United States;

(B) demonstrate a commitment to a career in higher education.

(8) CONSIDERATION.—In making selections for graduate traineeships under this paragraph, an institution receiving a grant under this subsection shall consider, to the extent possible, a diverse pool of applicants whose interests are of an interdisciplinary nature, encompassing the social scientific as well as the technical dimensions of cyber security.

(9) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this paragraph $5,000,000 for each of fiscal years 2003 through 2007.

SEC. 6. CONSULTATION.

In carrying out sections 4 and 5, the Director shall consult with other Federal agencies.

SEC. 7. FOSTERING RESEARCH AND EDUCATION IN COMPUTER AND NETWORK SECURITY.

Section 3(a) of the National Science Foundation Act of 1950 (42 U.S.C. 1862(a)) is amended—

(1) by striking ''and'' at the end of paragraph (6);

(2) by striking ''Congress.'' in paragraph (7) and inserting ''Congress ; and''; and

(3) by adding at the end the following:

''(8) to take a leading role in fostering and supporting research and education activities to improve the security of networked information systems.''.

SEC. 8. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY PROGRAMS.

(a) RESEARCH PROGRAM.—The National Institute of Standards and Technology Act (15 U.S.C. 271 et seq.) is amended—

(1) by moving section 22 to the end of the Act and redesignating it as section 32;

(2) by inserting after section 21 the following new section:

''SEC. 22. RESEARCH PROGRAM ON SECURITY OF COMPUTER SYSTEMS

''(a) ESTABLISHMENT.—The Director shall establish a program of assistance to institutions of higher education that enter into partnerships with for-profit entities to sup-

port research to improve the security of computer systems. The partnerships may also include government laboratories and nonprofit research institutions. The program shall—

''(1) include multidisciplinary, long-term research;

''(2) include research directed toward addressing needs identified through the activities of the Computer System Security and Privacy Advisory Board under section 20(f); and

''(3) promote the development of a robust research community working at the leading edge of knowledge in subject areas relevant to the security of computer systems by providing support for graduate students, post-doctoral researchers, and senior researchers.

''(b) FELLOWSHIPS.—

''(1) POST-DOCTORAL RESEARCH FELLOWSHIPS.—The Director is authorized to establish a program to award post-doctoral research fellowships to individuals who are citizens, nationals, or lawfully admitted permanent resident aliens of the United States and are seeking research positions at institutions, including the Institute, engaged in research activities related to the security of computer sys-

tems, including the research areas described in section 4(a)(1) of the Cyber Security Research and Development Act.

''(2) SENIOR RESEARCH FELLOWSHIPS.—The Director is authorized to establish a program to award senior research fellowships to individuals seeking research positions at institutions, including the Institute, engaged in research activities related to the security of computer systems, including the research areas described in section 4(a)(1) of the Cyber Security Research and Development Act. Senior research fellowships shall be made available for established researchers at institutions of higher education who seek to change research fields and pursue studies related to the security of computer systems.

''(3) ELIGIBILITY.—

''(A) IN GENERAL.—To be eligible for an award under this subsection, an individual shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require.

''(B) STIPENDS.—Under this subsection, the Director is authorized to provide stipends for post-doctoral research fellowships at the level of the Institute's Post Doctoral Research

Fellowship Program and senior research fellowships at levels consistent with support for a faculty member in a sabbatical position.

''(c) AWARDS; APPLICATIONS.—

''(1) IN GENERAL.—The Director is authorized to award grants or cooperative agreements to institutions of higher education to carry out the program established under subsection (a). No funds made available under this section shall be made available directly to any for-profit partners.

''(2) ELIGIBILITY.—To be eligible for an award under this section, an institution of higher education shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

''(A) the number of graduate students anticipated to participate in the research project and the level of support to be provided to each;

''(B) the number of post-doctoral research positions included under the research project and the level of support to be provided to each;

''(C) the number of individuals, if any, intending to change research fields and pursue studies related to the security of computer sys-

tems to be included under the research project and the level of support to be provided to each; and

''(D) how the for-profit entities, nonprofit research institutions, and any other partners will participate in developing and carrying out the research and education agenda of the partnership.

''(d) PROGRAM OPERATION.—

''(1) MANAGEMENT.—The program established under subsection (a) shall be managed by individuals who shall have both expertise in research related to the security of computer systems and knowledge of the vulnerabilities of existing computer systems. The Director shall designate such individuals as program managers.

''(2) MANAGERS MAY BE EMPLOYEES.—Program managers designated under paragraph (1) may be new or existing employees of the Institute or individuals on assignment at the Institute under the Intergovernmental Personnel Act of 1970, except that individuals on assignment at the Institute under the Intergovernmental Personnel Act of 1970 shall not directly manage such employees.

''(3) MANAGER RESPONSIBILITY.—Program managers designated under paragraph (1) shall be responsible for—

''(A) establishing and publicizing the broad research goals for the program;

''(B) soliciting applications for specific research projects to address the goals developed under subparagraph (A);

''(C) selecting research projects for support under the program from among applications submitted to the Institute, following consideration of—

''(i) the novelty and scientific and technical merit of the proposed projects;

''(ii) the demonstrated capabilities of the individual or individuals submitting the applications to successfully carry out the proposed research;

''(iii) the impact the proposed projects will have on increasing the number of computer security researchers;

''(iv) the nature of the participation by for-profit entities and the extent to which the proposed projects address the concerns of industry; and

''(v) other criteria determined by the Director, based on information specified for inclusion in applications under subsection (c); and

''(D) monitoring the progress of research projects supported under the program.

''(4) REPORTS.—The Director shall report to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Science annually on the use and responsibility of individuals on assignment at the Institute under the Intergovernmental Personnel Act of 1970 who are performing duties under subsection (d).

''(e) REVIEW OF PROGRAM.—

''(1) PERIODIC REVIEW.—The Director shall periodically review the portfolio of research awards monitored by each program manager designated in accordance with subsection (d). In conducting those reviews, the Director shall seek the advice of the Computer System Security and Privacy Advisory Board, established under section 21, on the appropriateness of the research goals and on the quality and utility of research projects managed by program managers in accordance with subsection (d).

''(2) COMPREHENSIVE 5-YEAR REVIEW.—The Director shall also contract with the National Research Council for a comprehensive review of the program established under subsection (a) during the 5th year of the program. Such review shall include an assessment of the scientific quality of the research conducted, the relevance of the research results obtained to the goals of the program established under subsection (d)(3)(A), and the progress of the program in promoting the development of a substantial academic research community working at the leading edge of knowledge in the field. The Director shall submit to Congress a report on the results of the review under this paragraph no later than 6 years after the initiation of the program.

''(f) DEFINITIONS.—In this section:

''(1) COMPUTER SYSTEM.—The term 'computer system' has the meaning given that term in section 20(d)(1).

''(2) INSTITUTION OF HIGHER EDUCATION.—The term 'institution of higher education' has the meaning given that term in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)).''.

(b) AMENDMENT OF COMPUTER SYSTEM DEFINITION.—Section 20(d)(1)(B)(i) of National Institute of Standards and Technology Act (15 U.S.C. 278g–3(d)(1)(B)(i)) is amended to read as follows:

"(i) computers and computer networks;".

(c) CHECKLISTS FOR GOVERNMENT SYSTEMS.—

(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the Federal government.

(2) PRIORITIES FOR DEVELOPMENT; EXCLUDED SYSTEMS.—The Director of the National Institute of Standards and Technology may establish priorities for the development of checklists under this paragraph on the basis of the security risks associated with the use of the system, the number of agencies that use a particular system, the usefulness of the checklist to Federal agencies that are users or potential users of the system, or such other factors as the Director determines to be appropriate. The Director of the National Institute of Standards and

Technology may exclude from the application of paragraph (1) any computer hardware or software system for which the Director of the National Institute of Standards and Technology determines that the development of a checklist is inappropriate because of the infrequency of use of the system, the obsolescence of the system, or the inutility or impracticability of developing a checklist for the system.

(3) DISSEMINATION OF CHECKLISTS.—The Director of the National Institute of Standards and Technology shall make any checklist developed under this paragraph for any computer hardware or software system available to each Federal agency that is a user or potential user of the system.

(4) AGENCY USE REQUIREMENTS.—The development of a checklist under paragraph (1) for a computer hardware or software system does not—

(A) require any Federal agency to select the specific settings or options recommended by the checklist for the system;

(B) establish conditions or prerequisites for Federal agency procurement or deployment of any such system;

(C) represent an endorsement of any such system by the Director of the National Institute of Standards and Technology; nor

(D) preclude any Federal agency from procuring or deploying other computer hardware or software systems for which no such checklist has been developed.

(d) FEDERAL AGENCY INFORMATION SECURITY PROGRAMS.—

(1) IN GENERAL.—In developing the agency-wide information security program required by section 3534(b) of title 44, United States Code, an agency that deploys a computer hardware or software system for which the Director of the National Institute of Standards and Technology has developed a checklist under subsection (c) of this section—

(A) shall include in that program an explanation of how the agency has considered such checklist in deploying that system; and

(B) may treat the explanation as if it were a portion of the agency's annual performance plan properly classified under criteria established by an Executive Order (within the meaning of section 1115(d) of title 31, United States Code).

(2) LIMITATION.—Paragraph (1) does not apply to any computer hardware or software system for which the National Institute of Standards and Technology does not have responsibility under section 20(a)(3) of the National Institute of Standards and Technology Act (15 U.S.C.278g-3(a)(3)).

SEC. 9. COMPUTER SECURITY REVIEW, PUBLIC MEETINGS, AND INFORMATION.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended by adding at the end the following new subsection:

''(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Secretary $1,060,000 for fiscal year 2003 and $1,090,000 for fiscal year 2004 to enable the Computer System Security and Privacy Advisory Board, established by section 21, to identify emerging issues, including research needs, related to computer security, privacy, and cryptography and, as appropriate, to convene public meetings on those subjects, receive presentations, and publish reports, digests, and summaries for public distribution on those subjects.''.

SEC. 10. INTRAMURAL SECURITY RESEARCH.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), as amended by this Act, is further amended by redesignating subsection (e)

as subsection (f), and by inserting after subsection (d) the following:

''(e) INTRAMURAL SECURITY RESEARCH.—As part of the research activities conducted in accordance with subsection (b)(4), the Institute shall—

''(1) conduct a research program to address emerging technologies associated with assembling a networked computer system from components while ensuring it maintains desired security properties;

''(2) carry out research associated with improving the security of real-time computing and communications systems for use in process control; and

''(3) carry out multidisciplinary, long-term, high-risk research on ways to improve the security of computer systems.''.

SEC. 11. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to the Secretary of Commerce for the National Institute of Standards and Technology—

(1) for activities under section 22 of the National Institute of Standards and Technology Act, as added by section 8 of this Act—

(A) $25,000,000 for fiscal year 2003;

(B) $40,000,000 for fiscal year 2004;

(C) $55,000,000 for fiscal year 2005;

(D) $70,000,000 for fiscal year 2006;

(E) $85,000,000 for fiscal year 2007; and

(2) for activities under section 20(f) of the National Institute of Standards and Technology Act, as added by section 10 of this Act—

(A) $6,000,000 for fiscal year 2003;

(B) $6,200,000 for fiscal year 2004;

(C) $6,400,000 for fiscal year 2005;

(D) $6,600,000 for fiscal year 2006; and

(E) $6,800,000 for fiscal year 2007.

SEC. 12. NATIONAL ACADEMY OF SCIENCES STUDY ON COMPUTER AND NETWORK SECURITY IN CRITICAL INFRASTRUCTURES.

(a) STUDY.—Not later than 3 months after the date of the enactment of this Act, the Director of the National Institute of Standards and Technology shall enter into an arrangement with the National Research Council of the National Academy of Sciences to conduct a study of the vulnerabilities of the Nation's network infrastructure and make recommendations for appropriate improvements. The National Research Council shall—

(1) review existing studies and associated data on the architectural, hardware, and software vulnerabilities and interdependencies in United States critical infrastructure networks;

(2) identify and assess gaps in technical capability for robust critical infrastructure network security and make recommendations for research priorities and resource requirements; and

(3) review any and all other essential elements of computer and network security, including security of industrial process controls, to be determined in the conduct of the study.

(b) REPORT.—The Director of the National Institute of Standards and Technology shall transmit a report containing the results of the study and recommendations required by subsection (a) to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Science not later than 21 months after the date of enactment of this Act.

(c) SECURITY.—The Director of the National Institute of Standards and Technology shall ensure that no information that is classified is included in any publicly released version of the report required by this section.

(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Secretary of Commerce for the National Institute of Standards and Technology for the purposes of carrying out this section, $700,000.

SEC. 13. COORDINATION OF FEDERAL CYBER SECURITY RESEARCH AND DEVELOPMENT

The Director of the National Science Foundation and the Director of the National Institute of Standards and Technology shall coordinate the research programs authorized by this Act or pursuant to amendments made by this Act. The Director of the Office of Science and Technology Policy shall work with the Director of the National Science Foundation and the Director of the National Institute of Standards and Technology to ensure that programs authorized by this Act or pursuant to amendments made by this Act are taken into account in any government-wide cyber security research effort.

SEC. 14. OFFICE OF SPACE COMMERCIALIZATION.

Section 8(a) of the Technology Administration Act of 1998 (15 U.S.C. 1511e(a)) is amended by inserting ''the Technology Administration of'' after ''within''.

SEC. 15. TECHNICAL CORRECTION OF NATIONAL CONSTRUCTION SAFETY TEAM ACT.

Section 2(c)(1)(d) of the National Construction Safety Team Act is amended by striking ''section 8;'' and inserting ''section 7;''.

SEC. 16. GRANT ELIGIBILITY REQUIREMENTS AND COMPLIANCE WITH IMMIGRATION LAWS.

(a) IMMIGRATION STATUS.—No grant or fellowship may be awarded under this Act, directly or indirectly, to

any individual who is in violation of the terms of his or her status as a nonimmigrant under section 101(a)(15)(F), (M), or (J) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(15)(F), (M), or (J)).

(b) ALIENS FROM CERTAIN COUNTRIES.—No grant or fellowship may be awarded under this Act, directly or indirectly, to any alien from a country that is a state sponsor of international terrorism, as defined under section 306(b) of the Enhanced Border Security and VISA Entry Reform Act (8 U.S.C. 1735(b)), unless the Secretary of State determines, in consultation with the Attorney General and the heads of other appropriate agencies, that such alien does not pose a threat to the safety or national security of the United States.

(c) NON-COMPLYING INSTITUTIONS.—No grant or fellowship may be awarded under this Act, directly or indirectly, to any institution of higher education or non-profit institution (or consortia thereof) that has—

(1) materially failed to comply with the record-keeping and reporting requirements to receive non-immigrant students or exchange visitor program participants under section 101(a)(15)(F), (M), or (J) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(15)(F), (M), or (J)), or section 641 of the Illegal Immigration Reform and Responsibility

Act of 1996 (8 U.S.C. 1372), as required by section 502 of the Enhanced Border Security and VISA Entry Reform Act (8 U.S.C. 1762); or

(2) been suspended or terminated pursuant to section 502(c) of the Enhanced Border Security and VISA Entry Reform Act (8 U.S.C 1762(c)).

SEC. 17. REPORT ON GRANT AND FELLOWSHIP PROGRAMS.

Within 24 months after the date of enactment of this Act, the Director, in consultation with the Assistant to the President for National Security Affairs, shall submit to Congress a report reviewing this Act to ensure that the programs and fellowships are being awarded under this Act to individuals and institutions of higher education who are in compliance with the Immigration and Nationality Act (8 U.S.C. 1101 et seq.) in order to protect our national security.

○